

REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed August 19, 2004. Upon entry of the amendments in this response, claims 1 – 2, 4 – 13, and 15 - 19 remain pending. In particular, Applicant has amended claims 1, 4, 8, 11, 15 – 16 and 18, and has canceled claims 3, 14 and 20 without prejudice, waiver, or disclaimer. Applicant has canceled claims 3, 14 and 20 merely to reduce the number of disputed issues and to facilitate early allowance and issuance of other claims in the present application. Applicant reserves the right to pursue the subject matter of these canceled claims in a continuing application, if Applicant so chooses, and does not intend to dedicate the canceled subject matter to the public. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

Rejections Under 35 U.S.C. §112, first paragraph

The Office Action indicates that claims 6 - 10 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enabling requirement. Applicant respectfully traverses the rejection.

Specifically, Applicant respectfully asserts that Applicants described the “data retrieval/encryption system” in such a way as to enable one skilled in the art to make and/or use the invention. In this regard, Applicant respectfully refers the Examiner’s attention to the following relevant portions of the specification that refer to the “data retrieval/encryption system”:

As shown in FIG. 1, secure printing system 10 can include one or more of a remote print system 100, *a data retrieval/encryption system 110 (“data system”)* and a print request system 120. Generally, remote print system 100 facilitates a secure printing operation by providing a user with information, *e.g.*, an encryption key, that can be used to encrypt data. The user can then provide the information to *data system 110*, such as via print request system 120, so that data that is intended for printing at the remote location can be

encrypted. Typically, such a **data system** is associated with the user's computer network and/or is otherwise associated with stored data that the user intends to print. By way of example, **data system 110** can be associated with a server 115 of the computer network. Regardless of the particular configuration utilized, the information to be printed can be encrypted and transmitted to the remote print system. Thereafter, the information can be decrypted and printed.

(Specification at page 5, lines 6 – 17). (Emphasis Added).

As mentioned before, encrypted information that is intended by a user to be decrypted and then printed, can be provided to a remote print system in various manners. **One such manner includes the use of a data retrieval/encryption system 110, such as that depicted in FIG. 1.** In one embodiment, **data system 110** is associated with the user's computer network, e.g., an office server.

Much like the remote print system described before, **data system 110** can be implemented in software, firmware, hardware, or a combination thereof. Preferably, **data system 110** is implemented in software as an executable program. As such, **data system 110** can be executed by a special or general purpose digital computer, such as a personal computer, work station, mini computer, or main frame computer. Typically, the **data system** is implemented by a server that is configured to receive inputs from and/or provide outputs to various devices, such as a personal digital assistant via a communication network. **An example of a computer that can implement data system 110 is shown schematically in FIG. 5.**

Generally, in terms of hardware architecture, computer 500 includes a processor 502, memory 504, and one or more input and/or output (I/O) devices 506 (or peripherals) that are communicatively coupled via a local interface 508. Software in memory 504 can include one or more separate programs, each of which comprises an ordered listing of executable instructions for implementing logical functions. In the embodiment of FIG. 5, the software in memory 504 includes **data system 110** and a suitable operating system (O/S) 510.

The functionality of a representative embodiment of the data system 110 is depicted in the flowchart of FIG. 6. As shown in FIG. 6, **data system** or method 110 may be construed as beginning at block 610 where input from a user is received. In block 620, information corresponding to the user input is identified. By way of example, the information corresponding to the user input can be information that the user intends to be printed as well as an encryption key, i.e., an encryption key provided by the remote print system. Thereafter, such as depicted in block 630, the identified information is enabled to be encrypted and, in block 640, the encrypted information is enabled to be provided to a communication network. More specifically, the encrypted information preferably is directed to a remote print system corresponding to a location where the user intends to have the information printed.

Functionality of an alternative embodiment of data system 110 is depicted in the flow chart of FIG. 7. As shown in FIG. 7, **data system** or method 110 may be construed as beginning at block 710 where information is enabled to be provided to a user. By way of example, the user could be

notified that information, such an email message, is available for printing. This information could be provided to the user via a portable computing device, such as a personal digital assistant or phone with messaging capability. In block 720, input from the user is received. Continuing with the previous example, when the user has been informed that information is available for printing, the user may be queried as to whether the user desires to print the available information. If an affirmative response is received, such as via the input of block 720, the user may be requested to provide an encryption key. The encryption key can be used by the *data system* for encrypting the information prior to transmission. In other embodiments, such as described hereinbefore in relation to the flowchart of FIG. 6, the user could provide information to the *data system* that facilitates identification of information to be printed as well as an encryption key. In such an embodiment, the user may not receive a notification that information is available for printing.

In block 730, the information to be printed is enabled to be encrypted using the encryption key provided by the user. Thereafter, such as depicted in block 740, the encrypted information is enabled to be provided, such as by directing the encrypted information to a remote print system.

Based on the foregoing, it should be appreciated that embodiments of the *data systems* of the invention can be adapted to identify information to be printed in response to a user input. In some instances, the user input can be prompted by the *data system*, which notifies the user that information is available for printing. Typically, a graphical user interface provided by a portable computing device of the user can be used to facilitate such a notification. In embodiments where a user is only able to request printing of information after being prompted by the *data system*, a user's portable computing device may not need to be particularly configured, *e.g.*, may not need to contain specific software, for interfacing with the *data system*. However, in those embodiments where a user is able to initiate the process of having information provided from a *data system* for printing, such a portable computing device may require particular adaptations. In particular, such a portable computing device may require the use of a print request system. A representative embodiment of a print request system 120 will now be described with reference to the schematic diagram of FIG. 8 and flowchart of FIG. 9.

(Specification, page 11, line 14 – page 14, line 7). (Emphasis Added).

The functionality of a representative embodiment of the print request system is depicted in the flowchart of FIG. 9. As shown in FIG. 9, print request system or method 120 may be construed as beginning at block 910 where an input is received. For instance, such an input may be provided from a user or, alternatively, from a *data retrieval/encryption system*. In block 920, a determination is made as to whether the user intends to print information corresponding to the input. If it is determined that the user does not desire to print the information, the information may be provided to the user. By way of example, the information may be displayed to the user via a display device of the portable computing device (depicted in block 930).

If however, it is determined that the user intends to print the information, the process may proceed to block 940.
(Specification, page 14, line 20 – page 15, line 5) (Emphasis Added).

Applicant respectfully asserts that the aforementioned portions of the written description and the associated accompanying figures not only satisfy the enablement requirement of 35 U.S.C. 112, first paragraph, these portions of the specification also recite various embodiments and alternative functionality of data retrieval/encryption systems. Applicant respectfully requests, therefore, that the rejection be withdrawn.

Rejections Under 35 U.S.C. §112, second paragraph

The Office Action indicates that claims 8 - 10 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to point out and distinctly claims the subject matter which applicant regards as the invention. As set forth above, Applicant has amended claim 8 such that is now depends from claim 6. Applicant respectfully asserts that the aforementioned amendment has rendered the rejection of claims 8 - 10 moot.

Rejections Under 35 U.S.C. §103

The Office Action indicates that claims 1 – 3, 11, 12, 14, 15 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Zingher* in view of *Maldy*. The Office Action further indicates that claims 4, 5, 13, 16, 17 and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Zingher* and *Maldy* in view of *Chomet*. The Office Action further indicates that claims 8 - 10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Zingher* in view of *Maldy* and *Barkan*. As set forth above, Applicant has canceled claims 3, 14 and 20, and respectfully asserts that the rejections as to these claims has been rendered moot. With respect to the remaining claims, Applicant respectfully traverses the rejections.

Turning first to *Zingher*, that reference generally involves a print job allocation system. As disclosed in *Zingher*, that reference teaches:

Using a printing plants profile generated from the data received from the printing machines 22 via the printing machine control devices 24 and the print job requirements profile generated from the data received from the data input devices 32, the print job processor 14 determines which printing machine(s) 22 in which printing plant(s) 20 are capable and available for processing a print job of the type input by the printing plant customer 30. Here, it is particularly important that the distribution requirements of the printed product, included in the requirements profile, are simultaneously taken into account when determining the optimum use of the printing machines 22 located throughout the world. Thus, as early as during the allocation of the print job for later dispatching of the print job, the distribution requirements of a print job are considered.

In the print job processor 14, the job requests entered by the customers 30 via the network 12 are compared against the free or available capacity input to the print job processor 14 via the printing machine control devices 24 of each of the printing plants 20. A particular print job is allocated and distributed to one or more printing plants 20 in accordance with the requirements profile generated from the data input by the customers 30 via the data input devices 32. As a result, each print job can be carried out in the best possible manner with regard to the optimization of time, material costs, desired quality and any other suitable criteria. (*Zingher*, col. 5, line 60 to col. 6, line 18).

Applicant respectfully asserts that, as shown in the exemplary teaching of *Zingher* above, *Zingher's* printing device is not involved with decryption of information that is to be printed. Additionally, *Zingher* discloses:

The data transmitted over the network 12 can be encrypted using known encryption devices and authentication codes, as desired, for security of data and to prevent tampering with print job requests or printing plant data. All of the data transmitted in the print job allocation system 10 may be encrypted for maximum security. Alternatively, various selected data transmissions in the print job allocation system 10 may be encrypted as desired. For example, it may be desirable to encrypt only data relating to print job requests and transmit the printing plant data in an unencrypted format. (*Zingher*, col. 3, lines 41 – 51).

Applicant also respectfully notes that *Zingher* has only disclosed using “known encryption devices and authentication codes,” for performing encryption. Thus, *Zingher* only teaches the use of a system other than a printing device for decrypting encrypted information

and only uses known encryption devices and authentication codes. This is in direct contrast to Applicant's claimed systems and methods as will be described in detail.

Additionally, Applicant respectfully asserts that none of the other cited references teaches or reasonably suggests the features/limitations described below as lacking in the combination of *Zingher* and *Maldy*. Therefore, Applicant respectfully asserts that the pending rejections are legally deficient for rendering the claims obvious under 35 U.S.C. § 103.

Turning to the claims, Claim 1 recites:

1. A secure printing system comprising:
a remote print system configured to provide a user with an encryption key, receive information encrypted using the encryption key, decrypt the information with a corresponding decryption key, and enable the information, once decrypted, to be printed; ***and***
a printing device configured to print hard copy the information;
wherein said remote print system is implemented by the printing device.
(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 1 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 1. Therefore, Applicant respectfully asserts that claim 1 is in condition for allowance. Since claims 2 and 4 - 10 are dependent claims that incorporate all the features/limitations of claim 1, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

With respect to Claim 11, that claim recites:

11. A secure printing system for printing information, the information being stored in memory at a location remote from a user, the information being accessible to the user via a communication network, said secure printing system comprising:
a remote print system arranged at a location remote from the information and configured to provide a user with an encryption key,

said remote print system being configured to communicate with the communication network such that said remote print system receives information encrypted using said encryption key,

said remote print system being further configured to decrypt said information with a corresponding decryption key, and enable said information, once decrypted, to be printed; and

a printing device configured to print hard copy of said information; wherein said remote print system is implemented by said printing device such that, once said information is decrypted using said decryption key, said printing device is enabled to print said information as hard copy.
(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 11 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 11. Therefore, Applicant respectfully asserts that claim 11 is in condition for allowance. Since claims 12 and 13 are dependent claims that incorporate all the features/limitations of claim 11, Applicant respectfully asserts that these claims also are in condition for allowance. Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

With respect to Claim 15, that claim recites:

15. A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

providing the user with an encryption key from a printing device;
receiving, at the printing device located at a second location remote from the first location, information encrypted using the encryption key via the communication network;

decrypting the information with a corresponding decryption key using the printing device; and

enabling the information, once decrypted, to be printed by the printing device.

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 15 unpatentable. In particular,

Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 15.

Therefore, Applicant respectfully asserts that claim 15 is in condition for allowance. Since claims 16 and 17 are dependent claims that incorporate all the features/limitations of claim 15, Applicant respectfully asserts that these claims also are in condition for allowance.

Additionally, these claims recite other features/limitations that can serve as an independent basis for patentability.

With respect to Claim 18, that claim recites:

18. A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

enabling an encryption key to be received from a printing device located at a second location remote from the first location;

enabling information that is to be printed to be identified; and

enabling the encryption key and information corresponding to the information that is to be printed to be transmitted to the first location via the communication network such that the information that is to be printed is encrypted using the encryption key, transmitted to the printing device located at the second location via the communication network, decrypted using a corresponding decryption key, and printed by the printing device.

(Emphasis Added).

Applicant respectfully asserts that the cited art, either individually or in combination, is legally deficient for the purpose of rendering claim 18 unpatentable. In particular, Applicant respectfully asserts that none of the references or combinations thereof teaches or reasonably suggests at least the features/limitations emphasized above in claim 18.

Therefore, Applicant respectfully asserts that claim 18 is in condition for allowance. Since claim 19 is a dependent claim that incorporates all the features/limitations of claim 18,

Applicant respectfully asserts that this claim also is in condition for allowance. Additionally, this claim recites other features/limitations that can serve as an independent basis for patentability.

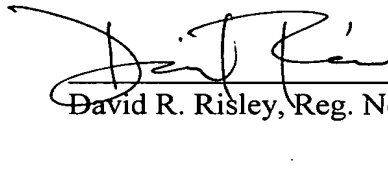
Cited Art Made of Record

The cited art made of record has been considered, but is not believed to affect the patentability of the presently pending claims.

CONCLUSION

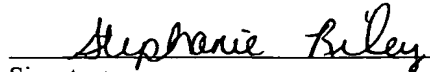
In light of the foregoing amendments and for at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,


David R. Risley, Reg. No. 39,345

**THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.**
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on 9/16/04.


Signature